

REMARKS

Applicant has reviewed the Final Office Action mailed November 30, 2006, and offers the following remarks.

Status of the Claims

Claims 1-35 are currently pending. No claims are added or cancelled by this response. Accordingly, claims 1-35 remain pending.

Rejection Under 35 U.S.C. § 103(a) - Bohnert and Ashton

Claims 1-6, 9, and 10 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,797,470 to Bohnert et al. (hereinafter "Bohnert") in view of U.S. Patent Application Publication No. 2004/0012567 A1 to Ashton (hereinafter "Ashton"). Applicant respectfully traverses. For the Patent Office to combine references in an obviousness rejection, the Patent Office must do two things. First, the Patent Office must establish *prima facie* obviousness by showing where each and every element is taught or suggested in the combined references. MPEP § 2143.03. Second, the Patent Office must state a motivation to combine the references. The motivation must be supported with actual evidence which cannot come from Applicant's disclosure. *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999).

Applicant respectfully submits that the Patent Office is still misinterpreting the cited references and is failing to consider elements of the claims that are not present within the cited references. Applicant hereby incorporates by reference the arguments presented within its Response to the Office Action mailed June 19, 2006 and filed on September 18, 2006 as if fully set forth herein. Applicant has further reviewed Bohnert and Ashton as requested by the Patent Office. Upon further review, Applicant respectfully submits that multiple elements of the claims are not taught by Bohnert or Ashton, either alone or in combination.

Prior to addressing the merits of the rejections, Applicant offers the following summary of an embodiment of the present invention. A depiction of the present invention as claimed is presented within Figures 9 through 11 of the present application. Figure 10 is reproduced herein to assist the Patent Office with understanding of the present invention.

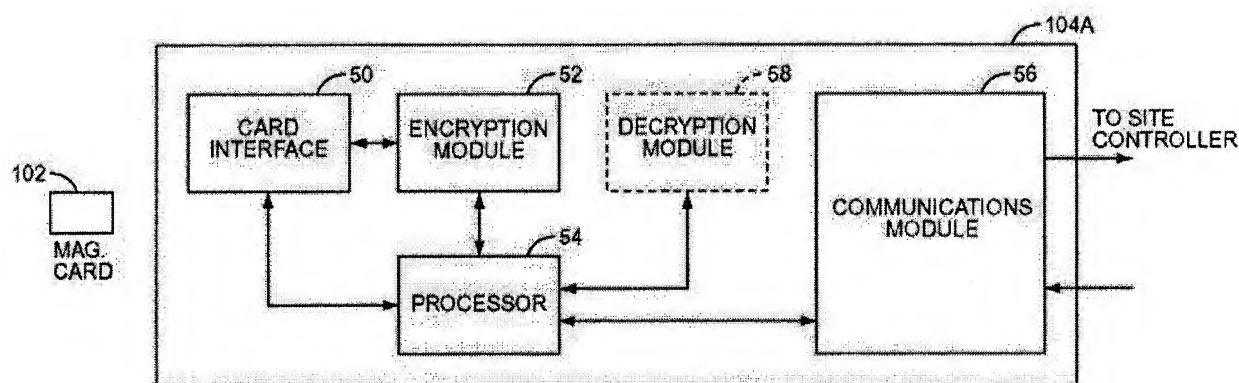


FIG. 10

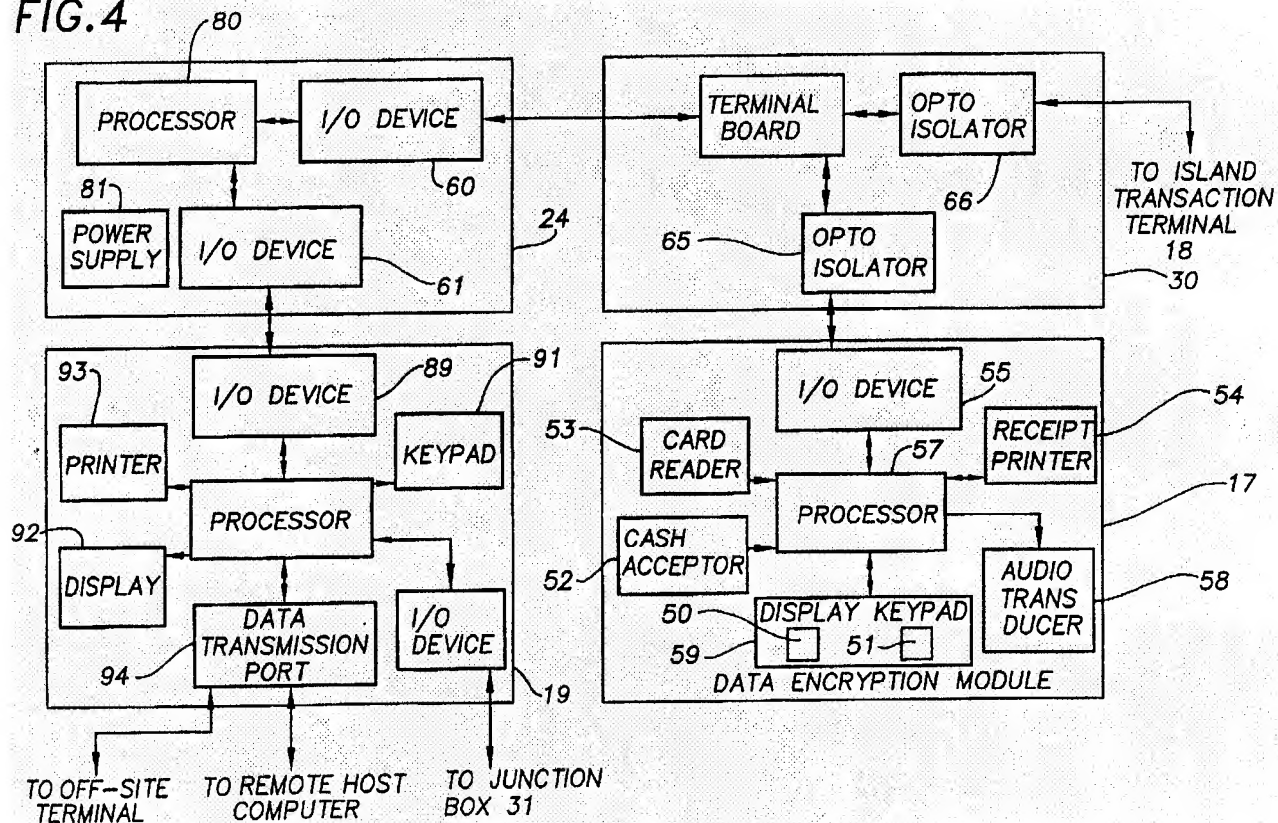
Figure 9 illustrates a fuel dispenser 140 that includes a card reader 104A and that is in communication with a site controller 110. The site controller 110 interfaces with a security module 112. Figure 10 illustrates that the card reader 104A includes an encryption module 52 and a communications module 56. The communications module 56 facilitates communication between the card reader 104A and both of the site controller 110 and the security module 112. Figure 11 illustrates that the card reader encrypts account information (step 1004). The card reader sends the encrypted account information to the site controller (step 1006). The security module then decrypts the account information received from the card reader and re-encrypts the account information for transfer to the authorization network (step 1008).

Claim 1 captures these components and characteristics by reciting a control system and security module that correlate, for example, with the site controller 110 and the security module 112 within Figure 9, respectively. Claim 1 also recites a card reader that correlates, for example, with the card reader 104A. The card reader is adapted to encrypt an account number received from a customer's card and to send the encrypted account number to the control system. In addition, claim 1 continues and recites that the security module decrypts the account number received from the card reader. As such, sending and receiving of the account number between a card reader that encrypts and sends an account number to a security module that receives and decrypts the received account number, respectively, are recited as elements within claim 1.

The Patent Office asserts that the encryption module 59 of Bohnert serves as a "security module" for encrypting the information entered by the user within the meaning of claim 1. (See Final Office Action mailed November 30, 2006, page 9, Response to Arguments). However, the

encryption module 59 of Bohnert is for encrypting a personal identification number (PIN) and not an account number. As such, the encryption module 59 of Bohnert cannot be a security module as claimed by Applicant. Figure 4 of Bohnert is reproduced herein to assist the Patent Office with recognition of the differences between Bohnert and the present invention.

FIG. 4



The Patent Office's interpretation of Bohnert is flawed for several reasons. First, as can be seen from Figure 4 of Bohnert, the encryption module 59 of Bohnert is associated with a transaction terminal 17 at a fuel dispenser that includes a display 50 and keypad 51. A card reader 53 is also associated with the fuel dispenser that is not at all associated with the encryption module 59, and thus the account number is not encrypted like in the claimed invention. The central master terminal 19 is shown as a separate unit and does not have a security module associated therewith. This encryption module 59 is used to encrypt a PIN number entered by the user via the keypad 51 at the fuel dispenser. The encrypted PIN number along with an unencrypted account number from the card reader are forwarded from the transaction terminal 17 to the central master terminal 19 for processing. The encryption module

59 never receives an encrypted account number from a card reader as required by claim 1. Second, because the encryption module 59 never receives an encrypted account number from a card reader, it naturally cannot decrypt an encrypted account number as is also required by claim 1. Thus, the encryption module 59 cannot serve as the “security module” of the claimed invention.

Also, the encryption module 59 cannot be found to be the “card reader” that encrypts the account number in the claims. While the encryption module 59 may perform an act of encrypting certain information, it does not send an encrypted account number to any module and does not send an encrypted account number to itself.

Claim 1 further recites that different components, namely the card reader and the security module, perform the encryption and decryption of the account number, respectively. Based upon this further distinction, a single module, such as the encryption module 59 of Bohnert, cannot be read on two different claim elements – to be both an encryption device for encryption of the account number and a decryption device to decrypt an account number within the meaning of claim 1, even given its broadest possible interpretation. Accordingly, the encryption module 59 of Bohnert cannot be the encrypting card reader or the security module that decrypts an encrypted account number that is received from the encrypting card reader as recited within claim 1 for at least these reasons.

The Patent Office further asserts that circuit 270 of Ashton serves as a security module based purely upon speculation that a module that is capable of encryption and decryption results in a security module within the meaning of claim 1. However, this interpretation of Ashton is also flawed for several reasons. First, the circuit 270 of Ashton never receives an encrypted account number from a card reader as required by claim 1. In fact, the circuit 270 actually receives an unencrypted account number from the card reader. Second, because the circuit 270 never receives an encrypted account number from a card reader, it cannot decrypt an encrypted account number received from a card reader as is also required by claim 1. Third, while the circuit 270 may perform an act of encrypting an account number, it does not transmit the encrypted account number to itself. Fourth, claim 1 further recites that different components, the card reader and the security module perform the encryption and decryption of the account number, respectively. Based upon this further distinction, a single module, such as the circuit 270 of Ashton, cannot be both an encryption device and a decryption device within the meaning

of claim 1, even given its broadest possible interpretation. Accordingly, the circuit 270 of Ashton cannot be both a card reader that encrypts an account number and a security module that decrypts an account number that is received from the card reader as recited within claim 1 for at least these reasons.

Accordingly, Applicant respectfully submits that these elements of Bohnert and Ashton are not security modules within the meaning of claim 1 even when giving claim 1 its broadest possible interpretation. There is no teaching within either Bohnert or Ashton, either alone or in combination, of a card reader sending an encrypted account number to a security module or of a security module decrypting an account number received from the card reader. Therefore, neither Bohnert nor Ashton, either alone or in combination, teach a security module as claimed. Further, neither teaches sending an encrypted account number from a card reader to a security module nor a security module that decrypts an account number received from a card reader. Accordingly, multiple elements of claim 1 are missing from the combination of references. For at least these reasons, the Patent Office has failed to properly form the present rejection and the rejection of claim 1 should be withdrawn.

Furthermore, the combination of Bohnert with Ashton teaches away from any combination of a card reader that encrypts an account number with a security module that locally decrypts an account number. Ashton, which is the only reference of the combination that refers to encryption of an account number, provides a stand-alone solution and does not indicate any need for local decryption of the account number. Ashton teaches encrypting an account number and communicating the encrypted account number directly to a merchant or credit card company over the Internet without decrypting or re-encrypting the account number. (See Ashton, paragraph 0026). As such, there is no motivation or suggestion within either Ashton or a combination of Ashton with Bohnert to locally decrypt an account number at a security module. Accordingly, the rejection of claim 1 should be withdrawn for these additional reasons.

Claims 2-6, 9, and 10 depend, either directly or indirectly, from claim 1. Accordingly, the rejection of claims 2-6, 9, and 10 should be withdrawn for at least the same reasons. Applicant respectfully submits that claims 1-6, 9, and 10 are in condition for allowance and notice of the same is requested at the earliest possible date.

Rejection Under 35 U.S.C. § 103(a) - Bohnert, Ashton, and Johnson

Claims 11, 12, 14-17, and 19-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bohnert as modified by Ashton as applied to claim 1, and further in view of U.S. Patent No. 5,384,850 to Johnson et al. (hereinafter "Johnson"). Applicant respectfully traverses. The standards for obviousness are set forth above.

Claims 11 and 12 depend, either directly or indirectly, from claim 1. As discussed above, claim 1 is allowable over the combination of Bohnert and Ashton. The addition of Johnson does not cure the deficiencies of Bohnert and Ashton. Accordingly, the rejection of claims 11 and 12 should be withdrawn for at least the same reasons as claim 1.

However, in order to provide a more comprehensive treatment of the deficiencies of the present rejection, Applicant offers the following additional comments. As discussed above, the combination of Bohnert and Ashton does not teach a security module as claimed. Johnson does not cure this deficiency. While Johnson does appear to teach a security module, the security module of Johnson only decrypts a personal identification number (PIN) and this PIN is received from a PIN pad. As such, the combination of Bohnert with Ashton and Johnson still does not teach a security module that receives an encrypted account number from a card reader that encrypts the account number. The combination also does not teach a security module that decrypts an encrypted account number received from a card reader. Additionally, the combination also does not teach a card reader that encrypts an account number and that sends the encrypted account number to the security module. As such, the combination of Bohnert and Ashton with Johnson still does not teach multiple elements of claim 1. Accordingly, the rejection of claims 11 and 12 should be withdrawn for these additional reasons.

Furthermore, the combination of Bohnert with Ashton and Johnson teaches away from any combination of a card reader that encrypts an account number with a security module that locally decrypts an account number. Ashton, which is the only reference of the combination that refers to encryption of an account number, provides a stand-alone solution and does not indicate any need for local decryption of the account number. Ashton teaches encrypting an account number and communicating the encrypted account number directly to a merchant or credit card company over the Internet without decrypting or re-encrypting the account number. (See Ashton, paragraph 0026). As such, there is no motivation or suggestion within either Ashton, or a combination of Ashton with Bohnert and Johnson, to locally decrypt an account number at a

security module. Accordingly, the rejection of claims 11 and 12 should be withdrawn for these additional reasons.

Claim 14 includes elements similar to those discussed above with respect to claim 1. Specifically, a communications module that is associated with a card reader device passes an encrypted account number to a site controller and a security module that is associated with the site controller decrypts the encrypted account number. A combination of Bohnert with Ashton and Johnson still does not teach these elements. Furthermore, as discussed above, a combination of Bohnert with Ashton and Johnson does not provide a motivation to locally decrypt an account number. In contrast, a combination of Bohnert with Ashton and Johnson teaches encryption of an account number at a card reader module and sending of the encrypted account number directly to a merchant or credit card company over the Internet without locally decrypting or re-encrypting the account number. As such, there is no motivation or suggestion within the references to locally decrypt or re-encrypt an encrypted account number. Accordingly, the rejection of claim 14 should be withdrawn for at least these reasons. Claims 15-17 depend, either directly or indirectly, from claim 14. Accordingly, the rejection of claims 15-17 should be withdrawn for at least the same reasons.

Claim 19 includes elements similar to those discussed above with respect to claims 1 and 14. Specifically, claim 19 recites sending an encrypted account number from a card reader to a site controller and decrypting the encrypted account number with a security module associated with the site controller. A combination of Bohnert with Ashton and Johnson still does not teach these elements. Furthermore, as discussed above, a combination of Bohnert with Ashton and Johnson does not provide a motivation to locally decrypt an account number. In contrast, a combination of Bohnert with Ashton and Johnson teaches encryption of an account number at a card reader module and sending of the encrypted account number directly to a merchant or credit card company over the Internet without locally decrypting or re-encrypting the account number. As such, there is no motivation or suggestion within the references to locally decrypt or re-encrypt an encrypted account number. Accordingly, the rejection of claim 19 should be withdrawn for at least these reasons. Claims 20-22 depend, either directly or indirectly, from claim 19. Accordingly, the rejection of claims 20-22 should be withdrawn for at least the same reasons.

Applicant respectfully submits that claims 11, 12, 14-17, and 19-22 are in condition for allowance and notice of the same is requested at the earliest possible date.

Rejection Under 35 U.S.C. § 103(a) - Bohnert, Ashton, Johnson, and Coppola

Claims 8, 18, 25, 26, 28, and 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bohnert as modified by Ashton and Johnson as applied to claims 1, 14, and 26, and further in view of U.S. Patent No. 6,360,138 B1 to Coppola et al. (hereinafter “Coppola”). Applicant respectfully traverses. The standards for obviousness are set forth above.

Claim 8 depends from claim 1, and claim 18 depends from claim 14. Claims 1 and 14 are clearly allowable over the combination of references cited and argued against above. Coppola does not cure the deficiencies of the combination of Bohnert with Ashton and Johnson. Accordingly, the rejection of claims 8 and 18 should be withdrawn for at least the same reasons.

Independent claim 25 includes similar limitations to those argued above as patentable in association with independent claims 1, 14, and 19. The combination of Bohnert, Ashton, Johnson, and Coppola still does not teach decrypting an account number at a secure module associated with a site controller, nor does the combination provide a motivation or suggestion to do so. Accordingly, the rejection of claim 25 should be withdrawn for at least the same reasons as those argued above in association with claims 1, 14, and 19. Further, dependent claims 26, 28, and 29 depend either directly or indirectly from claim 25. Accordingly, the rejection of claims 26, 28, and 29 should be withdrawn for at least the same reasons.

Applicant respectfully submits that claims 8, 18, 25, 26, 28, and 29 are in condition for allowance and requests notice of the same at the earliest possible date. Applicant need not address Coppola with respect to the added limitations in the rejected claims to overcome this rejection, but reserves the right to do so in the future, if required.

Rejection Under 35 U.S.C. § 103(a) - Bohnert, Ashton, Johnson, and Schneier

Claims 13 and 27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bohnert as modified by Ashton and Johnson as applied to claim 1, and further in view of “Applied Cryptography” pages 518-522 to Schneier (hereinafter “Schneier”). Applicant respectfully traverses. The standards for obviousness are set forth above.

Claims 13 and 27 depend either directly or indirectly from claims 1 and 25, respectively. Schneier does not cure the deficiencies of Bohnert with Ashton and Johnson. Accordingly, the rejection of claims 13 and 27 should be withdrawn for at least the same reasons as those argued above. Applicant respectfully submits that claims 13 and 27 are in condition for allowance and requests notice of the same at the earliest possible date. Applicant need not address Schneier with respect to the added limitations in the rejected claims to overcome this rejection, but reserves the right to do so in the future, if required.

Rejection Under 35 U.S.C. § 103(a) - Bohnert, Ashton, Johnson, and Campbell

Claims 7, 23, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bohnert as modified by Ashton and Johnson as applied to claims 1 and 19, and further in view of U.S. Patent No. 4,259,720 to Campbell (hereinafter "Campbell"). Applicant respectfully traverses. The standards for obviousness are set forth above.

Claims 7, 23, and 24 depend either directly or indirectly from claims 1 or 19. Campbell does not cure the deficiencies of Bohnert with Ashton and Johnson. Accordingly, the rejection of claims 7, 23, and 24 should be withdrawn for at least the same reasons as those argued above. Applicant respectfully submits that claims 7, 23, and 24 are in condition for allowance and requests notice of the same at the earliest possible date. Applicant need not address Campbell with respect to the added limitations in the rejected claims to overcome this rejection, but reserves the right to do so in the future, if required.

Claims Without Arguments from the Patent Office Formalizing a Rejection

Applicant has previously notified the Patent Office within its response filed September 18, 2006, that Applicant was not provided with arguments formalizing a rejection of claims 30-35 within the Office Action mailed June 19, 2006. Applicant further has not been provided with arguments formalizing a rejection of claims 30-35 within the Office Action mailed November 30, 2006. However, claims 30-35 depend either directly or indirectly from claims 1 and 14. Accordingly, the rejection of claims 30-35 should be withdrawn for at least the same reasons as those argued above. Applicant respectfully submits that claims 30-35 are in condition for allowance and requests notice of the same at the earliest possible date.

Conclusion

The present application is now in condition for allowance and such action is respectfully requested. The Examiner is encouraged to contact Applicant's representative regarding any remaining issues in an effort to expedite allowance and issuance of the present application.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By:

A handwritten signature in black ink, appearing to be 'S. Terranova', with a long horizontal line extending to the right.

Steven N. Terranova
Registration No. 43,185
P.O. Box 1287
Cary, NC 27512
Telephone: (919) 654-4520

Date: January 26, 2007
Attorney Docket: 2400-369A